

Developing Secure  
Web Applications

[日] 德丸浩 / 著 赵文 刘斌 / 译  
OWASP子明 / 审

# Web应用 安全 权威指南

日本Web应用安全第一人 **扛鼎力作!!**

OWASP北京区负责人、51CTO信息安全专家 **作序推荐**

—— 在虚拟机上亲自体验攻击流程 ——



人民邮电出版社  
POSTS & TELECOM PRESS

TURING

图灵程序设计丛书

Developing Secure  
Web Applications

[日] 德丸浩 / 著 赵文 刘斌 / 译  
OWASP子明 / 审

# Web应用 安全 权威指南

人民邮电出版社  
北京

## 图书在版编目(CIP)数据

Web应用安全权威指南 / (日) 德丸浩著; 赵文, 刘斌译. -- 北京: 人民邮电出版社, 2014.10  
(图灵程序设计丛书)  
ISBN 978-7-115-37047-1

I. ①W… II. ①德… ②赵… ③刘… III. ①网页制作工具 IV. ①TP393.092

中国版本图书馆CIP数据核字(2014)第206409号

*TAIKEITEKI NI MANABU ANZEN NA WEB APPLICATION NO TSUKURIKATA*

Copyright © 2011 HIROSHI TOKUMARU

All rights reserved.

Originally published in Japan by SB Creative Corp.

Chinese (in simplified characters only) translation rights arranged with

SB Creative Corp., Japan through CREEK&RIVER Co., Ltd.

本书中文简体字版由 SB Creative Corp. 授权人民邮电出版社独家出版。未经出版者书面许可, 不得以任何方式复制或抄袭本书内容。

版权所有, 侵权必究。

## 内 容 提 要

本书系日本 Web 安全第一人德丸浩所创, 是作者从业多年的经验总结。作者首先简要介绍了 Web 应用的安全隐患以及产生原因, 然后详细介绍了 Web 安全的基础, 如 HTTP、会话管理、同源策略等。此外还重点介绍了 Web 应用的各种安全隐患, 对其产生原理及对策进行了详尽的讲解。最后对如何提高 Web 网站的安全性和开发安全的 Web 应用所需要的管理进行了深入的探讨。本书可操作性强, 读者可以通过下载已搭建的虚拟机环境亲自体验书中的各种安全隐患。

本书适合 Web 相关的开发人员特别是安全及测试人员阅读。

- 
- ◆ 著 [日] 德丸浩
  - 译 赵文 刘斌
  - 审 OWASP 子明
  - 责任编辑 乐馨
  - 执行编辑 杜晓静
  - 责任印制 焦志炜
  - ◆ 人民邮电出版社出版发行 北京市丰台区成寿寺路11号  
邮编 100164 电子邮件 315@ptpress.com.cn  
网址 <http://www.ptpress.com.cn>  
北京鑫正夫印刷有限公司印刷
  - ◆ 开本: 800×1000 1/16  
印张: 25  
字数: 591千字 2014年10月第1版  
印数: 1-4000册 2014年10月北京第1次印刷  
著作权合同登记号 图字: 01-2014-0494号

---

定价: 79.00元

读者服务热线: (010)51095186 转 600 印装质量热线: (010)81055316

反盗版热线: (010)81055315

广告经营许可证: 京崇工商广字第 0021 号

## 推荐序

我投身信息安全产业领域已经有十五个年头了。过去我通过端口扫描，探测服务器的操作系统类型；防火墙出现后，我又转攻 Web 应用安全，结交了很多业内的顶级信息安全专家，与他们进行了大量的交流。

互联网的出现使得大家从传统的纸质信件传递转变为通过互联网电子邮件收发邮件；社交网络的出现，让我们得以通过互联网来结交更多的朋友。然而，我们在享受这些便利的同时，也承受着恶意钓鱼、跨站脚本攻击、恶意网马植入等风险。这些行为造成用户的信息泄漏，银行卡、信用卡信息被恶意盗刷，以致产生大量的经济损失。

通过国际权威的 Web 应用安全机构 OWASP 所发布的 TOP Ten，可以看出 Web 安全的重要性。现在全球有效的网络攻击中，基于 Web 的占 80%，SQL 注入与跨站脚本攻击一直都位于 OWASP Top Ten 的前两名，这两种攻击通常都发生在 Web 应用当中。

本次受图灵公司的邀请，参与了本书的校译工作，在进行校译期间看到了赵文和刘斌两位译者深厚的日文专业技术功底，同时也深深地感受到了日本人工作的严谨，作者在书中为大家准备了详实的应用案例和代码。

我作为 OWASP 中国北京的负责人，有幸组织和参与了在中国区域内召开的信息安全峰会与亚洲应用安全峰会，发现国外的信息安全专家更善于总结。他们能通过有效的方法论有效地进行一些精尖技术的推广和学习，而国内的信息安全专家在介绍一些高精技术时一般只告知结果，而不介绍过程。

《Web 应用安全权威指南》这本书的作者是日本 Web 安全第一人，足见其编程功底之深厚。本书没有欧美作者的那些诙谐幽默的用语，更多的是严谨而实用的陈述。作者以 Web 应用的安全隐患为引子，将产生安全隐患的原因作为整个主线来描述，同时还生动地介绍了试验这些安全隐患的环境的搭建，以及缺陷代码的示例。同时本书又给大家做了很好的补充说明，讲述了 Web 安全的基础协议和原理，帮助读者打好 Web 安全的基本功。

最难能可贵的是，本书详尽地讲解了 SQL 注入、XSS、CSRF 等的基本原理，同时又增加了详尽的代码解析。这是一本难得的 Web 应用安全指南。无论你是 Web 安全的爱好者，还是研究者，都可以将它作为一本很好的参考书籍。个人建议一些高校的学生通过学习本书，实现从 Web 安全的基础入门到精通。

OWASP 中国北京区负责人、51CTO 信息安全专家  
陈亮 (OWASP 子明)

## 译者序

2011年，索尼遭受了3次大规模攻击，造成7700万PlayStation Network（PSN）用户的个人信息泄漏。攻击令PSN网络服务瘫痪了23天，给索尼造成了上亿美元的经济损失。

2011年12月，国内知名开发者社区CSDN遭到攻击，600万用户账号及明文密码泄漏并在网络上被大量传播。

2013年3月，全球知名的云笔记应用Evernote遭到攻击，导致5000万用户的邮箱地址和加密密码泄漏。

写下这篇文章时，又正值全球最大的众筹网站Kickstarter被攻击而导致用户信息被窃取。

一件件触目惊心的事件无一不在提醒着我们网络安全的重要性。造成这些事件的罪魁祸首或许只是代码中一些不起眼的地方，但引发的影响及后果却骇人听闻。掌握如何在编程时不引入漏洞已成为了Web应用开发者不可或缺的技能。

然而，当开发者想要系统性地学习Web应用安全时，却发现市面上充斥着以攻击者的视角写作的“XX攻防大全”等书籍，却鲜有站在开发者立场的优秀的权威性书籍可供参考。图灵公司引进的这本《Web应用安全权威指南》正好填补了这一领域的空缺。

“在那本‘德丸本’中有透彻的讲解。”这是译者在日本工作期间，向同事询问“什么是CSRF”时得到的答复。没错，“德丸本”就是本书在日本的昵称，几乎在每个Web开发小组的案头都能发现它的身影。

本书的作者德丸浩先生在日本被誉为“Web应用安全领域第一人”，他在经营着一家Web安全咨询公司的同时，还在博客上笔耕不辍，孜孜不倦地分享着自己Web安全方面的知识，得此称号可谓实至名归。这本书是目前为止德丸浩先生出版的唯一一本图书，可以说是从业多年的经验沉淀下来的精华。

看过日系技术书的读者，一定会对其通俗易懂、深入浅出、谦虚谨慎等特点印象深刻，本书也不例外。SQL注入、XSS、CSRF等对于Web开发人员来说耳熟能详却可能一知半解的术语，都将在这本书中详细剖析。本书既适合从头到尾通读来进行系统性学习，也适合作为参考书时常查阅。

最后，再一次感谢图灵文化的编辑们能将这本书引入到国内。感谢另一位译者刘斌的辛勤付出，使得本书能够成功地问世。还要感谢妻子马超对我使用业余时间进行翻译工作的鼓励和支持。

希望本书能够让您受益。

赵文

2014年2月于无锡

# 前言

近年来，利用 Web 应用存在的安全隐患（即所谓的“漏洞”）展开攻击的案例层出不穷，受害者也与日俱增。虽说只要消除安全隐患就能够杜绝这些攻击，但这就需要 Web 应用开发人员掌握正确的安全性方面的知识。

目前，网络上充斥着大量关于安全性的信息，但多数内容都只是流于表面，无法解答开发人员的困惑。具体来说，主要存在以下几点疑问。

- 为什么会产生安全隐患
- 安全隐患会产生什么样的影响
- 如何编程才能消除安全隐患
- 为什么某些方法能够消除安全隐患

而本书就是为了解答这些疑问而创作的。为此，从安全隐患产生的原理到具体的对策，以及采用该对策的根据，本书都将尽可能地详细讲述。本书的目标读者包括程序员、设计师、项目经理、质量管理负责人等参与 Web 应用开发的全部人员。另外，本书也会站在 Web 应用的发包方（甲方）的立场上，尽可能地为其提供有用的信息。

虽然本书面向的是开发人员，但对攻击的手段也做了详细的解说。目的就是为了能够让读者切实感受到安全隐患所造成的影响。但有一点需要注意的是，如果没有得到网站管理员的许可就尝试实施攻击的话，就有可能触犯相关的法律法规。由于非专业人员很难判断自己的行为是否违法，因此，请不要在没有得到许可的情况下攻击正式的网站。

为了让读者能够放心地体验攻击流程，本书提供了在 VMware Player 的虚拟机环境中尝试安全隐患攻击的方法。希望读者能够通过亲自动手，来加深对安全隐患的理解。

最后，虽然本书中的示例代码主要使用了 PHP 语言，但讲述的内容对其他语言也是同样适用的。

# 谢辞

笔者在写作本书时，在网上征集了一些试读者，并根据试读者的意见和反馈不断地进行了调整。试读者不仅指出了错别字及语法问题，还提出了各种各样的改进方案，甚至还就安全隐患进行了深入的探讨，实在令笔者受益匪浅。如果没有这些建议和探讨，本书就不会是现在的样子。衷心感谢以下这些试读者（恕笔者省略敬称）：

大崎雅幸、太田良典、kaito834、加藤泰文、小邨孝明、坂井隆二、下冈叶子、高木正弘、竹迫良范、东内裕二、埴与志夫、日野洋一郎、山崎圭吾、山下太郎、Masahiro Yamada (masa141421356)、山本阳平

另外，长谷川阳介先生对本书提出了宝贵意见。同时笔者还在 Twitter 上收到了很多人士的建议。在此一并表示感谢。

最后还要感谢本书的编辑——SB Creative 股份有限公司信息书籍编辑部的友保健太先生，友保先生不仅对写作进度缓慢的笔者颇为照顾，还时常给出宝贵的意见和建议。在此向您致以衷心的感谢。

2011年1月  
德丸浩

# 目录

<b>第1章</b>	<b>什么是 Web 应用的安全隐患</b>	<b>1</b>
1.1	安全隐患即“能用于作恶的 Bug”	2
1.2	为什么存在安全隐患会有问题	3
	◆ 经济损失	3
	◆ 法律要求	3
	◆ 对用户造成不可逆的伤害	4
	◆ 欺骗用户	4
	◆ 被用于构建僵尸网络	4
1.3	产生安全隐患的原因	6
1.4	安全性 Bug 与安全性功能	7
1.5	本书的结构	8
<b>第2章</b>	<b>搭建试验环境</b>	<b>9</b>
2.1	试验环境概要	10
2.2	安装 VMware Player	11
	◆ 什么是 VMware Player	11
	◆ 下载 VMware Player	11
	◆ 安装 VMware Player	12
2.3	安装虚拟机及运行确认	14
	◆ 虚拟机启动确认	14
	◆ 虚拟机的使用方法	15
	◆ 编辑 hosts 文件	16
	◆ 使用 ping 确认连接	16
	◆ Apache 与 PHP 的运行确认	17
	◆ 设置并确认邮箱账号	17
2.4	安装 Fiddler	18
	◆ 什么是 Fiddler	18
	◆ 安装 Fiddler	18
	◆ Fiddler 的运行确认及简单用法	18



参考：虚拟机的数据一览	19
参考：如果无法连接试验环境的 POP3 服务器	20

## 第3章 Web 安全基础：HTTP、会话管理、同源策略 21

<b>3.1 HTTP 与会话管理</b>	22
为什么要学习 HTTP	22
最简单的 HTTP	22
◆ 使用 Fiddler 观察 HTTP 消息	23
◆ 请求消息	24
◆ 响应消息	24
◆ 状态行	25
◆ 响应头信息	25
◆ 如果将 HTTP 比喻为对话	25
输入 - 确认 - 注册模式	26
◆ POST 方法	28
◆ 消息体	28
◆ 百分号编码	29
◆ Referer	29
◆ GET 和 POST 的使用区别	29
◆ hidden 参数能够被更改	30
◆ 将 hidden 参数的更改比作对话	32
◆ hidden 参数的优点	32
无状态的 HTTP 认证	33
◆ 体验 Basic 认证	33
专栏 认证与授权	36
Cookie 与会话管理	36
◆ 使用 Cookie 的会话管理	39
◆ 会话管理的拟人化解说	39
◆ 会话 ID 泄漏的原因	42
◆ Cookie 的属性	42
专栏 Cookie Monster Bug	44
总结	45
<b>3.2 被动攻击与同源策略</b>	46
主动攻击与被动攻击	46
◆ 主动攻击	46
◆ 被动攻击	46
◆ 恶意利用正规网站进行的被动攻击	47
◆ 跨站被动攻击	48
浏览器如何防御被动攻击	48

◆ 沙盒	49
◆ 同源策略	49
◆ 应用程序安全隐患与被动攻击	52
专栏 第三方 JavaScript	53
JavaScript 以外的跨域访问	54
◆ frame 元素与 iframe 元素	54
专栏 X-FRAME-OPTIONS	54
◆ img 元素	54
◆ script 元素	54
◆ CSS	55
◆ form 元素的 action 属性	55
总结	56

## 第4章 Web 应用的各种安全隐患

57

4.1 Web 应用的功能与安全隐患的对应关系	58
安全隐患产生于何处	58
注入型隐患	59
总结	60
4.2 输入处理与安全性	61
什么是 Web 应用的输入处理	61
检验字符编码	62
转换字符编码	62
检验并转换字符编码的实例	62
专栏 字符编码的自动转换与安全性	64
输入校验	64
◆ 输入校验的目的	64
◆ 输入校验与安全性	65
◆ 二进制安全与空字节攻击	65
◆ 仅校验输入值并不是安全性策略	66
◆ 输入校验的依据是应用程序的规格	67
◆ 哪些参数需要校验	67
◆ PHP 的正则表达式库	67
◆ 使用正则表达式检验输入值的实例 (1) 1~5 个字符的字母数字	68
◆ 使用正则表达式检验输入值的实例 (2) 住址栏	70
专栏 请注意 mb_ereg 中的 \d 与 \w	70
范例	70
专栏 输入校验与框架	71
总结	72
参考: 表示“非控制字符的字符”的正则表达式	73

<b>4.3</b>	<b>页面显示的相关问题</b>	75
4.3.1	跨站脚本 (基础篇)	75
	概要	75
	攻击手段与影响	76
	◆ XSS 窃取 Cookie 值	76
	◆ 通过 JavaScript 攻击	79
	◆ 篡改网页	80
	◆ 反射型 XSS 与存储型 XSS	82
	安全隐患的产生原因	84
	◆ HTML 转义的概率	84
	◆ 元素内容的 XSS	85
	◆ 没有用引号括起来的属性值的 XSS	85
	◆ 用引号括起来的属性值的 XSS	85
	对策	86
	◆ XSS 对策的基础	86
	◆ 指定响应的字符编码	87
	◆ XSS 的辅助性对策	88
	◆ 对策总结	89
	参考: 使用 Perl 的对策示例	89
	◆ 使用 Perl 进行 HTML 转义的方法	89
	◆ 指定响应的字符编码	89
4.3.2	跨站脚本 (进阶篇)	90
	href 属性与 src 属性的 XSS	91
	◆ 生成 URL 时的对策	92
	◆ 校验链接网址	92
	JavaScript 的动态生成	92
	◆ 事件绑定函数的 XSS	92
	◆ script 元素的 XSS	94
	◆ JavaScript 字符串字面量动态生成的对策	95
	DOM based XSS	97
	允许 HTML 标签或 CSS 时的对策	99
	参考: Perl 中转义 Unicode 的函数	99
4.3.3	错误消息导致的信息泄漏	100
	总结	100
	继续深入学习	100
<b>4.4</b>	<b>SQL 调用相关的安全隐患</b>	101
4.4.1	SQL 注入	101
	概要	101
	攻击手段与影响	102
	◆ 示例脚本解说	102
	◆ 错误消息导致的信息泄漏	103

◆ UNION SELECT 致使的信息泄漏	104
◆ 使用 SQL 注入绕过认证	104
◆ 通过 SQL 注入攻击篡改数据	106
◆ 其他攻击	107
专栏 数据库中表名与列名的调查方法	108
安全隐患的产生原因	109
◆ 字符串字面量的问题	109
◆ 针对数值的 SQL 注入攻击	110
对策	110
◆ 使用占位符拼接 SQL 语句	111
专栏 采用 MDB2 的原因	111
◆ 为什么使用占位符会安全	111
◆ 参考: LIKE 语句与通配符	113
◆ 使用占位符的各种处理	114
◆ SQL 注入的辅助性对策	116
总结	117
继续深入学习	117
参考: 无法使用占位符时的对策	117
参考: Perl+MySQL 的安全连接方法	118
参考: PHP+PDO+MySQL 的安全连接方法	118
参考: Java+MySQL 的安全连接方法	118
<b>4.5 关键处理中引入的安全隐患</b>	120
4.5.1 跨站请求伪造 (CSRF)	120
概要	120
攻击手段与影响	121
◆ “输入 - 执行” 模式的 CSRF 攻击	121
◆ CSRF 攻击与 XSS 攻击	124
◆ 存在确认页面时的 CSRF 攻击	125
专栏 针对内部网络的 CSRF 攻击	127
安全隐患的产生原因	128
对策	129
◆ 筛选出需要防范 CSRF 攻击的页面	129
◆ 确认是正规用户自愿发送的请求	130
专栏 令牌与一次性令牌	131
◆ CSRF 的辅助性对策	133
◆ 对策总结	133
<b>4.6 不完善的会话管理</b>	134
4.6.1 会话劫持的原因及影响	134
◆ 预测会话 ID	134
◆ 窃取会话 ID	134
◆ 挟持会话 ID	135

◆ 会话劫持的方法总结 .....	135
◆ 会话劫持的影响 .....	135
4.6.2 会话 ID 可预测 .....	136
概要 .....	136
攻击手段与影响 .....	136
◆ 常见的会话 ID 生成方法 .....	136
◆ 使用推测出的会话 ID 尝试伪装 .....	137
◆ 伪装造成的影响 .....	137
安全隐患的产生原因 .....	137
对策 .....	138
◆ 改善 PHP 的会话 ID 的随机性的方法 .....	138
参考：自制会话管理机制产生的其他隐患 .....	139
4.6.3 会话 ID 嵌入 URL .....	139
概要 .....	139
攻击手段与影响 .....	140
◆ 会话 ID 嵌入 URL 所需的条件 .....	140
◆ 范例脚本解说 .....	141
◆ 通过 Referer 泄漏会话 ID 所需的条件 .....	142
◆ 攻击流程 .....	142
◆ 事故性的会话 ID 泄漏 .....	143
◆ 影响 .....	144
安全隐患的产生原因 .....	144
对策 .....	144
◆ PHP .....	144
◆ Java Servlet ( J2EE ) .....	145
◆ ASP.NET .....	145
4.6.4 固定会话 ID .....	145
概要 .....	145
攻击手段与影响 .....	146
◆ 示例脚本介绍 .....	146
◆ 会话固定攻击解说 .....	148
◆ 登录前的会话固定攻击 .....	148
◆ 会话采纳 .....	151
◆ 仅在 Cookie 中保存会话 ID 的网站固定会话 ID .....	151
◆ 会话固定攻击的影响 .....	151
安全隐患的产生原因 .....	152
对策 .....	152
◆ 无法更改会话 ID 时采用令牌 .....	153
◆ 登录前的会话固定攻击的对策 .....	154
总结 .....	154
<b>4.7 重定向相关的安全隐患 .....</b>	<b>155</b>

4.7.1	自由重定向漏洞	155
	概要	155
	攻击手段与影响	156
	安全隐患的产生原因	159
	◆ 允许自由重定向的情况	159
	对策	160
	◆ 固定重定向的目标 URL	160
	◆ 使用编号指定重定向的目标 URL	160
	◆ 校验重定向的目标域名	160
	专栏 警告页面	162
4.7.2	HTTP 消息头注入	162
	概要	162
	攻击手段与影响	163
	◆ 重定向至外部域名	165
	专栏 HTTP 响应截断攻击	166
	◆ 生成任意 Cookie	166
	◆ 显示伪造页面	168
	安全隐患的产生原因	170
	专栏 HTTP 消息头与换行	171
	对策	171
	◆ 对策 1: 不将外界参数作为 HTTP 响应消息头输出	171
	◆ 对策 2: 执行以下两项内容	171
	专栏 PHP 的 header 函数中进行的换行符校验	173
4.7.3	重定向相关的安全隐患总结	173
4.8	<b>Cookie 输出相关的安全隐患</b>	174
4.8.1	Cookie 的用途不当	174
	◆ 不该保存在 Cookie 中的数据	174
	◆ 参考: 最好不要在 Cookie 中保存数据的原因	174
	专栏 Padding Oracle 攻击与 MS10-070	176
4.8.2	Cookie 的安全属性设置不完善	176
	概要	176
	攻击手段与影响	177
	◆ 关于抓包方法的注意点	180
	安全隐患的产生原因	181
	◆ 什么样的应用程序不能在 Cookie 中设置安全属性	181
	对策	181
	◆ 给保存会话 ID 的 Cookie 设置安全属性的方法	182
	◆ 使用令牌的对策	182
	◆ 使用令牌能确保安全性的原因	184
	除安全属性外其他属性值需要注意的地方	184
	◆ Domain 属性	184

◆ Path 属性	185
◆ Expires 属性	185
◆ HttpOnly 属性	185
总结	185
<b>4.9 发送邮件的问题</b>	186
4.9.1 发送邮件的问题概要	186
◆ 邮件头注入漏洞	186
◆ 使用 hidden 参数保存收件人信息	186
◆ 参考：邮件服务器的开放转发	187
4.9.2 邮件头注入漏洞	187
概要	187
攻击手段与影响	188
◆ 攻击方式 1：添加收件人	190
◆ 攻击方式 2：篡改正文	191
◆ 通过邮件头注入攻击添加附件	192
安全隐患的产生原因	193
对策	194
◆ 使用专门的程序库来发送邮件	194
◆ 不将外界传入的参数包含在邮件头中	194
◆ 发送邮件时确保外界传入的参数中不包含换行符	195
◆ 邮件头注入的辅助性对策	195
总结	196
继续深入学习	196
<b>4.10 文件处理相关的问题</b>	197
4.10.1 目录遍历漏洞	197
概要	197
攻击手段与影响	198
专栏 从脚本源码开始的一连串的信息泄漏	200
安全隐患的产生原因	200
对策	201
◆ 避免由外界指定文件名	201
◆ 文件名中不允许包含目录名	201
专栏 basename 函数与空字节	202
◆ 限定文件名中仅包含字母和数字	202
总结	203
4.10.2 内部文件被公开	203
概要	203
攻击手段与影响	203
安全隐患的产生原因	204
对策	205

参考: Apache 中隐藏特定文件的方法	205
<b>4.11 调用 OS 命令引起的安全隐患</b>	206
4.11.1 OS 命令注入	206
概要	206
攻击手段与影响	207
◆ 调用 sendmail 命令发送邮件	207
◆ OS 命令注入攻击与影响	209
安全隐患的产生原因	210
◆ 在 Shell 中执行多条命令	210
◆ 使用了内部调用 Shell 的函数	211
◆ 安全隐患的产生原因总结	212
对策	212
◆ 在设计阶段决定对策方针	213
◆ 选择不调用 OS 命令的实现方法	213
◆ 避免使用内部调用 Shell 的函数	213
◆ 不将外界输入的字符串传递给命令行参数	216
◆ 使用安全的函数对传递给 OS 命令的参数进行转义	216
◆ OS 命令注入攻击的辅助性对策	217
参考: 内部调用 Shell 的函数	218
<b>4.12 文件上传相关的问题</b>	219
4.12.1 文件上传问题的概要	219
◆ 针对上传功能的 DoS 攻击	219
专栏 内存使用量与 CPU 使用时间等其他需要关注的资源	220
◆ 使上传的文件在服务器上作为脚本执行	220
◆ 诱使用户下载恶意文件	221
◆ 越权下载文件	222
4.12.2 通过上传文件使服务器执行脚本	222
概要	222
攻击手段与影响	223
◆ 示例脚本解说	223
专栏 警惕文件名中的 XSS	224
◆ PHP 脚本的上传与执行	224
安全隐患的产生原因	225
对策	225
专栏 校验扩展名时的注意点	228
4.12.3 文件下载引起的跨站脚本	228
概要	228
攻击手段与影响	229
◆ 图像文件引起的 XSS	229
◆ PDF 下载引起的 XSS	231



安全隐患的产生原因 .....	234
◆ 内容为图像时 .....	234
◆ 内容不为图像时 .....	235
对策 .....	236
◆ 文件上传时的对策 .....	236
专栏 BMP 格式的注意点与 MS07-057 .....	238
◆ 文件下载时的对策 .....	238
◆ 其他对策 .....	239
专栏 将图像托管在其他域名 .....	240
参考: 用户 PC 中没有安装对应的应用程序时 .....	240
总结 .....	241
<b>4.13 include 相关的问题</b> .....	242
4.13.1 文件包含攻击 .....	242
概要 .....	242
攻击手段与影响 .....	243
◆ 文件包含引发的信息泄漏 .....	244
◆ 执行脚本 1: 远程文件包含攻击 (RFI) .....	244
专栏 RFI 攻击的变种 .....	245
◆ 执行脚本 2: 恶意使用保存会话信息的文件 .....	246
安全隐患的产生原因 .....	248
对策 .....	248
总结 .....	248
<b>4.14 eval 相关的问题</b> .....	249
4.14.1 eval 注入 .....	249
概要 .....	249
攻击手段与影响 .....	250
◆ 存在漏洞的应用 .....	250
◆ 攻击手段 .....	252
安全隐患的产生原因 .....	253
对策 .....	253
◆ 不使用 eval .....	253
◆ 避免 eval 的参数中包含外界传入的参数 .....	254
◆ 限制外界传入 eval 的参数中只包含字母和数字 .....	254
◆ 参考: Perl 的 eval 代码块形式 .....	254
总结 .....	255
继续深入学习 .....	255
<b>4.15 共享资源相关的问题</b> .....	256
4.15.1 竞态条件漏洞 .....	256
概要 .....	256
攻击手段与影响 .....	257
安全隐患的产生原因 .....	258